Minnesota Journal of Law, Science & Technology

Volume 19 | Issue 2 Article 7

6-2018

No Good Deed Goes Unpunished: The Duties Held by Malware Researchers, Penetration Testers, and "White Hat" Hackers

Jon Watkins

Note

No Good Deed Goes Unpunished: The Duties Held by Malware Researchers, Penetration Testers, and "White Hat" Hackers

*Jon Watkins**

I. INTRODUCTION

More than five years ago, the National Security Agency (NSA) discovered a vulnerability[1] in Windows' implementation of SMBv1[2] and developed a tool, EternalBlue,[3] to exploit that

---

* JD Candidate 2019, University of Minnesota Law School; BA University of Minnesota, 2016. Thank you to Professor Ralph Hall for his feedback and guidance on this Note, to the editors and staff of MJLST for their phenomenal work, and to Martha, Maddie, Tom, and Mona for everything.

1. A "vulnerability" is an occurrence of a weakness (or multiple weaknesses) within software, in which the weakness can be used by a party to cause the software to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness.

CYBERSEC. UNIT, U.S. DEP'T JUST., A FRAMEWORK FOR A VULNERABILITY DISCLOSURE PROGRAM FOR ONLINE SYSTEMS 1 n.2 (2017).

2. Server Message Block (SMB) is the file protocol most commonly used by Windows. SMB Signing is a feature through which communications using SMB can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity. This security mechanism in the SMB protocol helps avoid issues like tampering of packets and "man in the middle" attacks.

Jose Barreto, *The Basics of SMB Signing*, MICROSOFT TECHNET (Dec. 1, 2010), https://blogs.technet.microsoft.com/josebda/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2/.

3. Ellen Nakashima & Craig Timberg, *NSA Officials Worried About the Day Its Potent Hacking Tool Would Get Loose. Then It Did*, WASH. POST (May 16, 2017), https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

vulnerability. The NSA used EternalBlue to surveil numerous targets with great success: as one former NSA employee said, using EternalBlue was "like fishing with dynamite."[4] Despite the NSA's awareness of EternalBlue's potency, the NSA withheld information about the underlying security vulnerability from Microsoft for years, perhaps fearing that the subsequent patch would destroy one of the NSA's most potent tools.[5]

The consequences of the decision to withhold this information became evident on April 14, 2017, when a group calling themselves Shadow Brokers released a massive trove of stolen NSA cyberweapons, including EternalBlue, to the public.[6] Initial reporting on the release focused heavily on EternalBlue and other vulnerabilities which appeared to be zero-day exploits[7] to which every Microsoft computer on the planet would be vulnerable.[8] This apocalyptic scenario—an uncontrolled cyberweapon capable of infiltrating the vast majority of computers on the planet[9]—turned out not to be the case, as Microsoft had released a security patch a month earlier,[10] but what actually happened is far from acceptable.

---

4. *Id.*

5. *See id.*

6. Dan Goodin, *NSA-Leaking Shadow Brokers Just Dumped Its Most Damaging Release Yet*, ARS TECHNICA (Apr. 14, 2017, 12:27 PM), https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/.

7. *See* Tony Bradley, *Zero Day Exploits*, LIFEWIRE (Oct. 19, 2016), https://www.lifewire.com/zero-day-exploits-2487435 ("A zero day exploit is when the exploit for the vulnerability is created before, or on the same day as the vulnerability is learned about by the vendor.").

8. *Id.*; *see also* Nicholas Weaver, *Shadow Brokers Redux: Dump of NSA Tools Gets Even Worse*, LAWFARE (Apr. 14, 2017, 12:31 PM), https://lawfareblog.com/shadow-brokers-redux-dump-nsa-tools-gets-even-worse.

9. Nicholas Weaver's response to the April 14 Shadow Brokers dump is representative of the attitude of many security professionals prior to learning the SMB vulnerability exploited by EternalBlue had been patched by Microsoft: "It really is a good weekend to turn off your computer." Weaver, *supra* note 8. The prospect of an unleashed cyberweapon so potent and so unexpected that the only safe response for even the information-security literate is to turn one's computer off—and leave it off until a patch is available—should rightly be considered terrifying.

10. Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack*, MICROSOFT: MICROSOFT ON THE ISSUES (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/; *see also* Goodin, *supra* note 6; Weaver, *supra* note 8.

On May 12, 2017, less than a month after EternalBlue was publicly released, EternalBlue was used as a means of spreading Wannacry, the now-infamous malware that locked computers in 150 countries,[11] caused up to $4 billion in losses,[12] and crippled the UK's National Health Service (NHS).[13] Even though EternalBlue was by this point in time harmless to Windows computers as long as the owner had applied the security patch released two months earlier,[14] immense numbers of computers remained unpatched, and were therefore vulnerable.[15]

EternalBlue and Wannacry represent a unique set of problems at the intersection of cybersecurity and law: did the NSA have a responsibility to disclose the underlying SMB vulnerability to Microsoft? Would the discoverer of that vulnerability have had the same responsibility if it were not the NSA, but instead a civilian, or a company which competes with Microsoft? If any of these parties had such a responsibility, did it arise when the vulnerability was first discovered? When EternalBlue was stolen? Shadow Brokers are frequently portrayed as a malicious actor in the story of Wannacry, but what is it that makes their actions malicious? Is it because they stole tools from the NSA? Is it because they allegedly released zero-days and cyberweapons to the public? Is it because they did not contact Microsoft in advance of the public release? Is it something else entirely?

These questions are important, and many of them have no sufficient answer or analogy in existing law. This Note will attempt to address some of them, although addressing all of them would be an immense undertaking which is outside the scope of this Note. After addressing these questions and other critical issues brought up by the current state of vulnerability research and malware development, this Note concludes that individuals who develop malware or discover software vulnerabilities must be held to prevailing standards of

---

11. Jonathan Berr, *"WannaCry" Ransomware Attack Losses Could Reach $4 Billion*, CBS: MONEYWATCH (May 16, 2017, 5:00 AM), https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

12. *Id.*

13. Owen Hughes, *WannaCry Impact on NHS Considerably Larger than Previously Suggested*, DIGITAL HEALTH (Oct. 27, 2017), https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/.

14. Smith, *supra* note 10.

15. *Id.*

disclosure, which must be developed and revised in cooperation with a variety of stakeholders. The currently prevailing standards, including Responsible Disclosure, are detailed at length below. When individuals violate their duties as laid out by these standards, they should be held civilly, or in rare cases criminally, liable for their actions.

II. BACKGROUND

A. WHAT ARE VULNERABILITIES, AND WHY DO THEY MATTER?

Software can be very difficult to design. The software behind a commonly used website or application can include anywhere from ten thousand to ten million lines of code, and all of Google's Internet Service code combined amounts to over 2 billion lines of code.[16] While the ideal world may include software without vulnerabilities, the sheer scale of much software means such a world is not quite within our reach.[17] Various groups have drastically differing approaches to vulnerabilities. Government actors like the NSA have an established practice of stockpiling vulnerabilities rather than helping vendors remedy them.[18] This approach is highly effective at achieving national security

16. *Codebases*, INF. IS BEAUTIFUL (Sept. 24, 2015), https://informationisbeautiful.net/visualizations/million-lines-of-code/.

17. Marian K. Riedy & Bartlomiej Hanus, *It Is Just Unfair Using Trade Laws to "Out" Security Software Vulnerabilities*, 48 LOY. U. CHI. L.J. 1099, 1099 (2017) ("All but the simplest software contains some vulnerabilities, including coding errors.").

18. Russell Brandom, *After Shadow Brokers, Should the NSA Still Be Hoarding Vulnerabilities?*, VERGE (Aug. 19, 2016, 9:53 AM), https://www.theverge.com/2016/8/19/12548462/shadow-brokers-nsa-vulnerability-disclosure-zero-day. *But see* THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 219 (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (advocating for an end to the NSA stockpiling policy, and arguing the NSA should aid vendors in patching vulnerabilities).

objectives[19] and at committing lucrative cybercrime,[20] but is not effective at protecting individual consumers or companies.[21]

Additionally, the line between vulnerabilities and malware may be very thin: a demonstration of a vulnerability sufficient to either sell that vulnerability or publicly disclose it generally includes a proof of concept, and a proof of concept is, in turn, typically very close in form to an exploit, which would be salable as malware.[22] For this reason, "malware" and "vulnerability" will be used more or less interchangeably in this paper. While they are conceptually different for programming purposes, this difference has a negligible effect on how each should be disclosed to the public.[23]

---

19. Mailyn Fidler, Anarchy or Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities 11 (May 2014) (unpublished B.A. thesis, Stanford University) (on file with Stanford University), https://stacks.stanford.edu/file/druid:zs241cm7504/Zero-Day%20Vulnerability%20Thesis%20by%20Fidler.pdf ("The inclusion of zero-days in Stuxnet demonstrates their high value to the U.S. government for offensive cyber operations.").

20. Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, 19 ACM CONF. ON COMPUTER & COMMS. SECURITY 833, 833 (2012), https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf ("For cyber criminals, unpatched vulnerabilities in popular software, such as Microsoft Office or Adobe Flash, represent a free pass to any target they might wish to attack, from Fortune 500 companies to millions of consumer PCs around the world.").

21. *See* Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 793 (2016) ("[E]very zero day that is secretly used by a government is one more zero day that can be used against that government's law-abiding citizens, either by that government or by someone else.").

22. *Id.* at 802 ("Vulnerability sales often require proof of concept, in which case the seller will have to build a working exploit. At that time, the seller is faced with another choice because he or she now has the start of a product, the exploit, which could demand a high price on the black market.").

23. Generally, the tech world uses "vulnerability" to refer to security flaws in systems, and "malware" or "exploit" to refer to intentional exploitation of that flaw. *Id.* at 759. Despite that important technical distinction, this paper focuses mostly on the disclosure duty and other duties held by various parties, and those duties rarely change due to this distinction. The distinction may be an especially critical distinction in a negligence lawsuit focusing on causation, for instance, but discussing vulnerabilities and malware separately in this paper would result in substantial redundancy. Finally, this Note is not entirely alone in opting to give less weight to this distinction in the context of duty. Clause 7.2 of ISO/IEC 29147, for example, states that while proofs of concept are sensitive information, vendors have a general duty to provide a secure means to submit all vulnerability reports, whether or not they include a proof of concept in addition to information about the vulnerability. INT'L ORG. FOR

Tech companies have a vested interest in producing secure software, and fixing vulnerabilities in their software as soon as possible. While many tech companies run bug bounty programs which pay large amounts of money to third parties who find and disclose vulnerabilities in the company's code,[24] these sums of money may be dwarfed by the amount the vulnerability could fetch on the black market,[25] and some tech companies have a practice of suing researchers who discover vulnerabilities in their software—a practice which may heavily discourage disclosure.[26] Some researchers may also opt to publicly disclose the vulnerability, with or without the cooperation of the software vendor.[27] The decision to publicly disclose a vulnerability often comes with substantial risks.[28] Despite these risks, public disclosure is very popular, possibly because, as Kesan and Hayes note: "Reputation is practically a currency in the information security field. Being known as the person who discovered a major security flaw might prove as valuable as being paid in legal

---

STANDARDIZATION & INT'L ELECTROTECHNICAL COMM., VULNERABILITY DISCLOSURE: ISO/IEC 29147 § 7.2 (2014).

24. *See, e.g.*, *Chrome Reward Program Rules*, GOOGLE, https://www.google.com/about/appsecurity/chrome-rewards/ (last visited Apr. 14, 2018) ("Rewards for qualifying bugs typically range from $500 to $100,000. We have a standing $100,000 reward for participants that can compromise a Chromebook or Chromebox with device persistence in guest mode.").

25. *See* Kesan & Hayes, *supra* note 21, at 761 ("Unfortunately, bug bounties are often just a fraction of what the researcher could earn if he or she sold the information to someone else."); Robert Hackett, *Jailbreaks Wanted: $1 Million Dollar iPhone Hacks*, FORTUNE (Sept. 21, 2015), http://fortune.com/2015/09/21/ios9-million-dollar-hack/ ("The cybersecurity firm Zerodium announced on Monday that it will reward $1 million to anyone able to crack Apple's recently launched iOS 9 operating system, which the startup's website claims is 'the world's most secure mobile OS.'").

26. Kesan & Hayes, *supra* note 21, at 789. For a more recent example, see Zack Whittaker (@zackwhittaker), TWITTER (Mar. 21, 2018, 5:06 PM), https://twitter.com/zackwhittaker/status/976611110223835137, which describes a recent lawsuit brought by a tech company against security researchers and a news website regarding technicalities in the disclosure of a security vulnerability in the tech company's product.

27. Kesan & Hayes, *supra* note 21, at 793–94.

28. *Compare* Bilge & Dumitras, *supra* note 20, at 2 ("After zero-day vulnerabilities are disclosed, the number of malware variants exploiting them increases 183–85,000 times and the number of attacks increases 2–100,000 times."), *with* Kesan & Hayes, *supra* note 21, at 793 ("Zero days are valuable on the open market . . . as long as they remain unknown to others . . . . This aspect of zero days may be one reason why many security researchers prefer to publicly disclose vulnerabilities. By shedding light on the vulnerability, the value of the vulnerability to malicious actors plummets.").

currency."[29] For this reason, safeguards on disclosure are sometimes cast aside in the pursuit of recognition.[30] There are, of course, non-fame-related reasons to publicly disclose a vulnerability,[31] but these justifications may not be empirically sound.[32]

This point brings us to the central questions of this paper—what are the specific legal duties of cybersecurity professionals with regards to disclosure? What safeguards need to exist to ensure proper disclosure, and to ensure that vulnerabilities are handled properly? How can any given system differentiate between malicious, benign, and beneficial actors, and should

---

29. Kesan & Hayes, *supra* note 21, at 794. Some infrastructure does exist for providing the types of reward and recognition which may well be currency to a security researcher, and often couples that reward with actual currency. This infrastructure includes BugCrowd and HackerOne, both of which are recommended by I Am The Cavalry. *BugCrowd*, BUGCROWD, https://www.bugcrowd.com/ (last visited Apr. 14, 2018); *HackerOne*, HACKERONE, https://www.hackerone.com/ (last visited Apr. 14, 2018); *I Am the Cavalry Position on Disclosure*, I AM THE CAVALRY (June 25, 2014), https://www.iamthecavalry.org/about/disclosure/. Other bug bounty programs, including Google's, also personally name researchers who discover certain classes of vulnerabilities—providing another avenue for the desired recognition. *See, e.g.*, *Chrome Reward Program Rules*, *supra* note 24.

30. An example may help to illustrate this point. Recently, a security researcher allegedly discovered a possibly enormous vulnerability—unauthorized root access—within Mac OS X Sierra, and published the vulnerability on Twitter, apparently without contacting Apple first. Lemi Orhan Ergin (@lemiorhan), TWITTER (Nov. 28, 2017, 10:38 PM), https://twitter.com/lemiorhan/status/935578694541770752 ("Anyone can login as 'root' with empty password after clicking on login button several times."). One account's response was representative of widespread condemnation of this disclosure: "QA failures notwithstanding: there's no need to set an entire street afire in order to point out that the kitchen in one house is burning." Blacklight (@blacklightpix), TWITTER (Nov. 28, 2017, 2:46 PM), https://twitter.com/blacklightpix/status/935641138987286528.

31. Google Security Team, *Rebooting Responsible Disclosure: A Focus on Protecting End Users*, GOOGLE SEC. BLOG (July 20, 2010), https://security.googleblog.com/2010/07/rebooting-responsible-disclosure-focus.html ("[T]he argument for full disclosure proceeds: because a given bug may be under active exploitation, full disclosure enables immediate preventative action, and pressures vendors for fast fixes. Speedy fixes, in turn, make users safer by reducing the number of vulnerabilities available to attackers at any given time.").

32. *See, e.g.*, Bilge & Dumitras, *supra* note 20 ("After zero-day vulnerabilities are disclosed, the number of malware variants exploiting them increases 183–85,000 times and the number of attacks increases 2–100,000 times."); Google Security Team, *supra* note 31 ("We understand that not all bugs can be fixed in 60 days, although many can and should be.").

such a differentiation change the duties that attach to any given actor?[33] Questions of duty and liability are especially important in the cybersecurity context, because as Kesan and Hayes note: "systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail."[34] In other words, consumer information may only be secure when the corporations keeping that information in a vault, and the hackers holding the keys to that vault, are both subject to liability when something goes wrong. Under standard theories of negligence, this liability can only arise where a standard of care or duty exists.[35]

B. WHAT DUTIES ARISE IN SIMILAR CONTEXTS?

A general duty to behave in a manner which is not unreasonably dangerous attaches to nearly everyone, nearly all the time.[36] There is no general duty to prevent harm caused by the criminal acts of others,[37] but such a duty can arise due to certain relationships or in certain contexts—for example, the duty to protect one's patients can be strong enough to overcome even therapist/client privilege.[38] This duty to safeguard, and other duties to prevent harm to third parties, are limited by intervening causes.[39] Intervening causes do not always sever liability, especially where the harm caused by the intervention was reasonably foreseeable.[40] However, when considering cases

---

33. For a complex discussion of the types of individuals involved in malware research, hacking, and related fields, see Kesan & Hayes, *supra* note 21, at 769 (adapting the Dungeons and Dragons Morality/Ethics framework to cybersecurity).

34. *Id.* at 780 (quoting Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCI., Oct. 27, 2006, at 610).

35. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 7 cmt. a (AM. LAW INST. 2010).

36. Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334, 342 (Cal. 1976) (quoting Rodriguez v. Bethlehem Steel Corp, 525 P.2d 669, 680 (Cal. 1974)) ("As a general principle, a 'defendant owes a duty of care to all persons who are foreseeably endangered by his conduct, with respect to all risks which make the conduct unreasonably dangerous.'").

37. Bridges v. Parrish, 742 S.E.2d 794, 796 (N.C. 2013).

38. *Tarasoff*, 525 P.2d at 345.

39. Kush v. City of Buffalo, 449 N.E.2d 725, 729 (N.Y. 1983).

40.

> [A]n intervening intentional or criminal act will generally sever the liability of the original tort-feasor, but, on the facts here, [Defendant] may not rely on this doctrine.

involving less foreseeable acts, which may include criminal acts, courts may be more likely to find that an intervening cause does sever liability.[41]

Specifically considering the disclosure of dangerous information, restrictions on disclosure have been established in disciplines other than cybersecurity, and are often premised on the logic that certain information is too dangerous to be disclosed publicly. One example is the 2011 H5N1 (avian flu) publication debate, which resulted in publication,[42] but also in an

---

> That doctrine has no application when the intentional or criminal intervention of a third party or parties is reasonably foreseeable . . . . When the intervening, intentional act of another is itself the foreseeable harm that shapes the duty imposed, the defendant who fails to guard against such conduct will not be relieved of liability when that act occurs.

Id. (holding that a city was not freed of liability under intervening cause doctrine where chemicals were insufficiently stored at a school, a child subsequently lit the chemicals on fire, and was injured); *see also* Herrera v. Quality Pontiac, 73 P.3d 181, 194 (N.M. 2003) (finding that leaving a key in the ignition of an unattended, unlocked car in a high-crime area owes a duty of ordinary care to individuals injured in an auto accident when a thief steals the car, even where the auto accident was criminally caused by the thief, because the theft and accident were foreseeable).

41. *See* Wilken v. City of Lexington, 754 N.W.2d 616, 621–24 (Neb. Ct. App. 2008) (holding that an intervening cause severed liability where a police officer had left an unrestrained prisoner and a loaded shotgun in his running vehicle, and the prisoner subsequently shot the plaintiffs with said shotgun); Johnstone v. City of Albuquerque, 145 P.3d 76, 85 (N.M. Ct. App. 2006) (holding that a stepfather was not liable for juvenile's suicide where said suicide was not foreseeable, despite the stepfather's failure to significantly safeguard his gun).

42. Michael J. Imperiale & Arturo Casadevall, *A New Synthesis for Dual Use Research of Concern*, PLOS MED., Apr. 14, 2015, at 2, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4397073/pdf/pmed.1001813.pdf (describing the debate over publication of the Kawaoka and Fouchier papers, which described how a strain of avian influenza could be made transmissible by air). Due to concerns that the contents of certain research papers could be used for bioterror, many members of the scientific community, as well as the U.S. Government, became involved in a protracted debate about whether or not the papers could be published, and if so, whether the papers could be redacted. *Id.* NSABB (the National Science Advisory Board for Biosecurity) recommended that the portion of the paper consisting essentially of "instructions" should not be published, although the end results of the research were sufficiently significant to merit publication. *Id.* This finding was supported by the dominant calculus for publication review in this context—the Dual Use Research of Concern (DURC) Policy, originally published in 2007. NAT'L SCI. ADVISORY BD. FOR BIOSEC., PROPOSED FRAMEWORK FOR THE OVERSIGHT OF DUAL USE LIFE SCIENCES RESEARCH: STRATEGIES FOR MINIMIZING THE POTENTIAL MISUSE OF RESEARCH INFORMATION 15 (2007). NSABB's position was contradicted by the U.S. Government, which forced NSABB to vote on either full publication or no

extensively considered grant of power to the U.S. government to restrict publication of Dual-Use Research of Concern (DURC), as well as a straightforward calculus for when publication should be restricted.[43] As another example, nuclear weapons are not patentable,[44] primarily because nuclear weapons are too dangerous to be publicly disclosed as the U.S. patent system requires.[45] However, most analogous restrictions on disclosure outside of those tied to privilege law[46] use existing oversight mechanisms such as the Patent and Trademark Office (PTO) or the National Science Advisory Board for Biosecurity (NSABB), instead of imposing a legal duty on the individual holding the sensitive information.[47]

Finally, deviating slightly from the discussion of duty, existing strict liability torts merit some consideration here. Generally speaking, "abnormally dangerous activities" are subject to strict liability rather than a conventional negligence analysis—examples of such activities include certain illegal

---

publication—the papers were eventually published in full. Imperiale & Casadevall, *supra*, at 2.

43. *See* Imperiale & Casadevall, *supra* note 42, at 3. "[Federal Agencies may] [*r*]*equest voluntary redaction* of the research publications or communications[;][*c*]*lassify the research*, in accordance with National Security Decision Directive/NSDD-189[; or] [n]ot provide or *terminate research funding*." Franca R. Jones, *Dual Use Research of Concern: The March 29 Policy*, NAT'L SCI. ADVISORY BOARD FOR BIOSECURITY (Nov. 27, 2012), https://osp.od.nih.gov/wp-content/uploads/2013/12/NSABB_Meeting_Jones_March_29_Policy_slides%20(1).pdf (emphasis in original).

44. 42 U.S.C. § 2181 (2012). Note, however, § 2181(a): "No patent shall hereinafter be granted for any invention or discovery which is useful *solely* in . . . an atomic weapon." *Id.* (emphasis added). "Solely" invites a comparison to dual-use research as described in note 42, as it implies that nuclear-related patents which have a second use are not necessarily excluded under that provision. Even though § 2181(a) predates the DURC policy by 71 years, it implies the same policy foundation: there should be a presumption of disclosure where some public benefit inheres in certain information, even if malicious actors could misuse that information.

45. ROBERT PATRICK MERGES & JOHN FITZGERALD DUFFY, PATENT LAW AND POLICY 206–07 (7th. ed. 2017).

46. *See* Tarasoff v. Regents of University of California, 551 P.2d 334, 347 (1976) ("We conclude that the public policy favoring protection of the confidential character of patient-psychotherapist communications must yield to the extent to which disclosure is essential to avert danger to others. The protective privilege ends where the public peril begins."); *see also* Upjohn Co. v. U.S., 449 U.S. 383, 389 (1981) ("The attorney-client privilege is the oldest of the privileges for confidential communications known to the common law.") (citing 8 J. WIGMORE, EVIDENCE § 2290 (McNaughton rev. 1961)).

47. *E.g.* Imperiale & Casadevall, *supra* note 42 and accompanying text.

fireworks displays and the transportation of explosive material.[48] Under such an analysis, whether the defendant exercised a reasonable standard of care is irrelevant. The Restatement definition of "abnormally dangerous" is critical in such cases—it applies strict liability only to activities which are uncommon, and which "[create] a foreseeable and highly significant risk of physical harm even when reasonable care is exercised by all actors."[49] As will be discussed below, there is a colorable argument that vulnerability and malware research is abnormally dangerous, which would render the strict liability analysis highly relevant.

C. WHAT DUTIES ARISE DUE TO CYBERSECURITY LEGISLATION AND INDUSTRY NORMS?

The U.S. government has attempted to bring clarity to cybersecurity law in recent years. The National Institute of Standards and Technology (NIST) recently provided voluntary cybersecurity standards,[50] but said standards only infrequently mention disclosure or the proper means of handling vulnerabilities and malware. The Cybersecurity Information Sharing Act (CISA)[51] permits voluntary sharing of "cyber threat indicators and defensive measures,"[52] and provides a shield from antitrust liability where cybersecurity information is shared between private entities for cybersecurity purposes,[53] but providing a shield for certain voluntary conduct does not necessarily establish a duty to perform that conduct, and CISA was also mostly targeted at large companies, rather than individual researchers or small groups of researchers.[54]

---

48. *See, e.g.*, JAMES A. HENDERSON, JR., RICHARD N. PEARSON & DOUGLAS A. KYSAR, THE TORTS PROCESS 464 (8th ed. 2012).

49. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 (AM. LAW INST. 2010). Notably, there are other ways in which strict liability can be applied to a certain situation, including, for example, possessing exotic or dangerous pets. *Id.*, §§ 22–23. Other situations in which strict liability applies are, however, outside the scope of this paper.

50. *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

51. 6 U.S.C. §§ 1501–10 (Supp. 2016).

52. Kesan & Hayes, *supra* note 21, at 773.

53. 6 U.S.C. § 1503(e) (Supp. 2012).

54. *See* Eric Geller, *Your Complete Guide to CISA, the Cybersecurity Bill Scaring Privacy Activists*, DAILY DOT (Dec. 11, 2015, 9:38 AM), https://www

Furthermore, the mere existence of voluntary standards has been criticized,[55] which calls the standards stated in both the CISA and the NIST into question. Further cybersecurity legislation has been discussed which would more directly deal with vulnerability and malware disclosure through treating malware as a weapon subject to arms control,[56] but its future is uncertain. Additionally, similar to the DURC discussion in the context of H5N1 above, many cybersecurity tools (including some encryption technologies) are considered dual-use goods under the Wassenaar Agreement, an international "voluntary export control regime," but the Agreement has little controlling force, as it is not technically a treaty.[57] Finally, for a discussion of the Computer Fraud and Abuse Act (CFAA), see Part D below.

In addition to the legislation discussed above, discussions surrounding industry norms[58] for vulnerability and malware disclosure abound. Kesan and Hayes note that public disclosures of vulnerabilities are commonly made at industry conferences, and that "[t]he current prevailing norm is to work with the vendor ahead of time to ensure that the vulnerability is patched before the presentation."[59] However, substantial debate exists regarding precisely how much notice is appropriate, and whether researchers may publicly disclose vulnerabilities at

---

.dailydot.com/layer8/what-is-cisa-2015-s754-cybersecurity-information-sharing-act/.

55. *E.g.*, Kesan & Hayes, *supra* note 21, at 776 ("Some critics question the wisdom of even voluntary cybersecurity standards, due to the risk that companies will adopt the bare minimum required to comply. Providing a higher baseline than what might have existed before is valuable, but the danger comes when agencies mistake practices that are necessary to improve security, and practices that are sufficient to improve security.").

56. *See, e.g.*, John Reed, *The U.S. Senate Wants to Control Malware Like It's a Missile*, FOREIGN POL'Y (June 27, 2013, 6:35 PM), http://foreignpolicy.com/2013/06/27/the-u-s-senate-wants-to-control-malware-like-its-a-missile/ (describing one such bill).

57. Kesan & Hayes, *supra* note 21, at 777. The Wassenaar Agreement, which is essentially aimed at harmonizing export controls on conventional weapons and DURC technology (see section B, *supra*, for a more in-depth discussion of DURC), has been viewed as a tool for controlling the zero-day vulnerability market. *See* Fidler, *supra* note 19, at 135.

58. The benefits of using industry norms to determine the direction of cybersecurity law are substantial. *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1154 (2016) (comparing judicial analysis in the realm of virtual trespass to that of a "Martian from outer space," and asserting that "[w]ithout established norms to rely on, the application of a seemingly simple concept like 'authorization' becomes surprisingly hard").

59. Kesan & Hayes, *supra* note 21, at 794.

conferences to pressure a vendor to patch a vulnerability, where researchers believe the vendor has unduly delayed the patch.[60] Additionally, lively debate exists regarding the ethics of any sort of public disclosure,[61] and researchers who rely on being able to monetize their discoveries may find themselves disappointed by the size of the bug bounty they may or may not receive from a vendor, in the context of the payments they could receive on the grey or black market from a government or other entity who would effectively pay the researcher *not* to publicly disclose the vulnerability.[62]

For researchers who are less interested in their bank accounts, Responsible Disclosure[63] is an appealing model, which essentially requires that researchers give vendors a certain period of prior warning before they release information about a vulnerability publicly. Some Responsible Disclosure models rely on cooperation with trusted third parties to delay disclosure by a reasonable time frame.[64] Nearly all Responsible Disclosure models allow for the date of public disclosure to be adjusted based on the severity of the vulnerability, as well as the needs of both the vendor and the researcher.[65] A number of parties have extensively advocated for Responsible Disclosure and attempted to provide incentives for researchers to participate,[66] but concerns about appropriate compensation persist, especially

---

60. *Id.* at 793–94.

61. *See id.* at 794–95 ("Disclosure is thus a double-edged sword, increasing the likelihood of attacks while simultaneously supporting improvements in security."); Bilge & Dumitras, *supra* note 20, at 842 ("[T]he participants to the debate disagree about whether trading off a high volume of attacks for faster patching provides an overall benefit to the society.").

62. *See* Kesan & Hayes, *supra* note 21, at 761 ("Unfortunately, bug bounties are often just a fraction of what the researcher could earn if he or she sold the information to someone else.").

63. *See* Douglas Bonderud, *The Responsible Disclosure Policy: Safeguard or Cybercriminal Siren Song?*, SECURITY INTELLIGENCE (Dec. 26, 2014), https://securityintelligence.com/the-responsible-disclosure-policy-safeguard-or-cybercriminal-siren-song/.

64. *E.g.* US-CERT, DEP'T OF HOMELAND SEC., INFO SHEET**,** https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf ("To protect America's cyberspace, US-CERT . . . [a]cts as a trusted third-party to assist in the responsible disclosure of vulnerabilities.").

65. Google Security Team, *supra* note 31.

66. *E.g.* Kesan & Hayes, *supra* note 21, 803 (citing Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1086 (2011)) ("Bambauer and Day, for example, recommend granting researchers immunity from intellectual property litigation if they follow a responsible disclosure model.").

where the researcher discovers a vulnerability in the software of a vendor who does not offer bug bounties.[67] Proposals like Coordinated Vulnerability Disclosure (CVD) are highly similar to Responsible Disclosure, and have much the same effect.[68]

Some authors have focused their proposals away from researchers, and toward vendors. Recent litigation has sparked some discussion of a duty to safeguard in the cybersecurity context, although the cases to date have mainly focused on the duty of companies to safeguard personally identifiable information,[69] and the extent to which intervening causes sever liability related to that duty.[70] Some authors have also argued that vendors have a duty to write safe and vulnerability-free code,[71] although this duty seems practically impossible to

---

67. Many companies' responsible disclosure policies expressly foreclose the possibility of any compensation at all, and some explicitly threaten a lawsuit will follow a request for compensation. *E.g.*, *Tricentis Flood Security*, FLOOD BY TRICENTIS, https://flood.io/security (last visited Apr. 14, 2018) ("Tricentis reserves all of its legal rights in the event of any noncompliance . . . Requests for monetary compensation in connection with any identified or alleged vulnerability will be deemed noncompliant with this Responsible Disclosure Policy."). *See generally* Fahmida Y. Rashid, *Facebook Joins Google, Mozilla, Barracuda in Paying Bug Bounties*, EWEEK (Aug. 3, 2011), http://www.eweek.com/blogs/security-watch/facebook-joins-google-mozilla-barracuda-in-paying-bug-bounties.

68. *See*, *e.g.*, Chris Betz, *A Call for Better Coordinated Vulnerability Disclosure*, MICROSOFT TECHNET (Jan. 11, 2015), https://blogs.technet.microsoft.com/msrc/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure/.

69. *See, e.g.*, *In re* Yahoo! Inc. Customer Data Security Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *27 ("The crux of Plaintiffs' allegations is not that Defendants safeguards failed to be '100% secure.' Rather, the crux of Plaintiffs' allegations is that Defendants' safeguards did not comply with applicable laws and regulations and that Defendants' data encryption protocol was 'widely discredited and had been proven, many years prior, easy to break.'").

70. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 246 (3d Cir. 2015) (citing RESTATEMENT (SECOND) OF TORTS § 449 (AM. LAW INST. 1965)) ("If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act[,] whether innocent, negligent, intentionally tortious, or criminal[,] does not prevent the actor from being liable for harm caused thereby.").

71. *See* Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 137 (2010); Paul N. Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. & POL'Y REV. 239, 251–52 (2013).

fulfill.[72] Additionally, both the International Organization for Standardization (ISO) vulnerability disclosure standard[73] and Department of Justice (DOJ) vulnerability disclosure framework[74] focus heavily on vendors, while the ISO standard explicitly excludes researchers, and the DOJ framework largely fails to assign them duty.[75]

Finally, it should be noted that the U.S. government is frequently the party responsible for researching and managing vulnerabilities, and substantial debate exists regarding various proposals to limit the US government's ability to stockpile vulnerabilities.[76] While sovereign immunity and related doctrines are outside the scope of this Note, it should be mentioned that many proposals have been put forward regarding limiting the ability of the U.S. government to retain vulnerabilities,[77] although many authors doubt the U.S. government is likely to ever give up the ability to use and stockpile cyberweapons.[78] These national security implications

---

72. *See* Riedy & Hanus, *supra* note 17 ("All but the simplest software contains some vulnerabilities, including coding errors.").

73. INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM., *supra* note 23, at v.

74. CYBERSEC. UNIT, U.S. DEP'T JUST., *supra* note 1, at 1.

75. While the DOJ Framework does point out that one incentive to create a vulnerability disclosure program is reducing the possibility of inadvertent violations of the CFAA, this portion of the Framework does not create any new duties, nor does it really interpret existing duties under the CFAA. *Id.* at 1–2, 1 n.3. Instead, it aims to aid organizations in clarifying what access is "authorized" and what is not, since "exceeding authorized access" may result in a CFAA violation. *Id.* at 1–2.

76. *See, e.g.*, Smith, *supra* note 10 ("[W]e called in February for a new 'Digital Geneva Convention' to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.").

77. *See, e.g.*, Weaver, *supra* note 8 ("This dump also provides significant ammunition for those concerned with the [U.S.] government developing and keeping 0-day exploits. Like both previous Shadow Brokers dumps, this batch contains vulnerabilities that the NSA clearly did not disclose even after the tools were stolen. This means either that the NSA can't determine which tools were stolen—a troubling possibility post-Snowden—or that the NSA was aware of the breach but failed to disclose to vendors despite knowing an adversary had access. I'm comfortable with the NSA keeping as many 0-days affecting U.S. systems as they want, so long as they are NOBUS (Nobody But Us). Once the NSA is aware an adversary knows of the vulnerabilities, the agency has an obligation to protect U.S. interests through disclosure.").

78. *See* David E. Sanger, *Nations Seek the Elusive Cure for Cyberattacks*, N.Y. TIMES (Jan. 21, 2018), https://mobile.nytimes.com/2018/01/21/business/davos-international-cyberattack-prevention.html ("The United

complicate analyses of the WannaCry/Shadow Brokers fact pattern which introduced this Note—while under ordinary principles, a duty may have existed for any private company to share this information with Microsoft, the need for effective national security tools may be a sufficiently strong countervailing interest to justify the NSA's sustained failure to inform Microsoft of the SMB vulnerability exploited by EternalBlue.[79]

D. WHAT CRIMINAL LAWS APPLY TO MALWARE RESEARCHERS?

The primary U.S. criminal law involving hacking is the Computer Fraud and Abuse Act (CFAA),[80] which may have been enacted partially in response to *War Games*, a 1983 Cold War-themed movie about hackers.[81] Generally speaking, "the CFAA criminalized exceeding authorized access to a protected computer system."[82] The CFAA has been unevenly applied[83] and roundly criticized,[84] but remains highly significant in this field and in others.[85] Recent litigation involving the CFAA has drawn

---

States, for example, would never support rules that banned espionage . . . . It is a power that the United States and its allies, have no intention of giving up.").

79. For more in-depth discussion of the national security implications posed by NSA cyberweapon stockpiles, see Weaver, *supra* note 8, and Sanger, *supra* note 78.

80. 18 U.S.C. § 1030 (2012); *see* Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. REV. 383, 392 (2014).

81. *See* Kirsch, *supra* note 80.

82. *Id.*

83. Kesan & Hayes, *supra* note 21, at 771 ("[S]ome question the government's enforcement patterns. A majority of referred CFAA cases are left unprosecuted due to lack of evidence, while CFAA prosecutions that do go forward sometimes play fast and loose with what it means to access a computer without authorization.").

84. *See* Kirsch, *supra* note 80, at 392–93 ("[A]ll hacking is essentially illegal under the [CFAA] . . . . the CFAA has become so broad that the law now 'threatens to swallow the Internet.' . . . . The broad language of the CFAA is a result of out-dated Internet philosophies from before the Internet's omnipresence in society."); Kesan & Hayes, *supra* note 21, at 771 ("[I]nconsistent applications of [CFAA] threaten to discourage benevolent security research while encouraging the actions of malicious hackers who know that their odds of being caught and prosecuted are slim."); Fidler, *supra* note 19, at 68 ("The CFAA has been criticized for its 'breadth and severity.' The law has increasingly been used to prosecute offenses . . . . one might not consider classical hacking.").

85. WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 472 (Robert C. Clark et al. eds., 2016) ("[T]he use of the CFAA has evolved and a large proportion of current litigation under the law—both criminal and civil—

substantial ire from the security community,[86] but in the context of vulnerability disclosure, at least one court has remarked that merely publicly disclosing a vulnerability is not a CFAA violation,[87] in a case that attracted significant attention among security researchers and computer scientists.[88] The DOJ recently publicized guidelines on CFAA prosecution,[89] which shed light on the Department's thought process with regard to the modern applicability of the CFAA: for the most part, the Department is interested in prosecuting cases in which sensitive information was accessed, or a "pillar of society," such as public health or major infrastructure, is threatened by the access.[90]

Finally, since virtually any crime can be committed online,[91] crimes as serious as homicide may be committed as well. Given the breadth of the CFAA as discussed above, and at least one

---

now involves the misappropriation of confidential business information or trade secrets.").

86. Kirsch, *supra* note 80, at 386–87 (discussing the facts of *U.S. v. Auernheimer*, as well as the response to the verdict, which was "heavily criticized by security professionals" as making "the rest of us less safe").

87. Kesan & Hayes, *supra* note 21, at 795 (citing Mass. Bay Transp. Auth. v. Anderson, No. 1:08-CV-11364(GAO), 2008 WL 6954925 (D. Mass. Jan. 26, 2009)) ("Some vendors have attempted to argue that the act of publicly disclosing a vulnerability or exploit is a violation of computer crime law, but no court has officially ruled on this question. In 2008, the [MBTA] sued three MIT students to prevent them from giving a presentation at a conference that included information about a vulnerability in MBTA's ticketing system. The court denied MBT"'s request for a preliminary injunction and remarked that it was unlikely that MBTA's claim would succeed on the merits.").

88. Brief of Amici Curiae Computer Science Professors and Computer Scientists, Mass. Bay Transp. Auth. v. Anderson, No. 1:08-CV-11364(GAO), 2008 WL 6954925 (D. Mass. Jan. 26, 2009).

89. Memorandum from the Attorney Gen. to the U.S. Attorneys and Assistant Attorney Gens. for the Criminal and Nat'l Sec. Div., Intake and Charging Policy for Computer Crime Matters (Sept. 11, 2014), https://www.justice.gov/criminal-ccips/file/904941/download [hereinafter Attorney General Memorandum].

90. Jenna McLaughlin, *Justice Department Releases Guidelines on Controversial Anti-Hacking Law*, INTERCEPT (Oct. 26, 2016, 11:30 AM), https://theintercept.com/2016/10/26/justice-department-releases-guidelines-on-controversial-anti-hacking-law/. The importance of these "pillars" is also reflected in the existence of the 16 "Sector Coordinating Councils"—information-sharing organizations with the goal of protecting critical sectors of the American economy who receive high-clearance security information from the U.S. government, from the private sector, and from each other. *See Sector Coordinating Councils*, DHS (July 11, 2017), https://www.dhs.gov/scc.

91. Susan W. Brenner, *Nanocrime?*, 2011 U. ILL. J.L. TECH. & POL'Y 39, 60–71 (2011) (describing a vast array of crimes committed through the use of computers).

general definition of involuntary manslaughter,[92] unintentionally causing the death of an individual while accessing any digital platform without authorization (which is the core of conduct criminalized by the CFAA, even though other elements beyond unauthorized access are necessary to proving a crime) may be prosecutable as involuntary manslaughter. This is somewhat comparable to law which existed before the digital era: involuntary manslaughter has been found in the context of a duty to safeguard.[93] While no one as yet appears to have died directly due to malware or similar attacks, such a death may be an inevitability given the frequency of attacks on healthcare systems.[94] The DOJ CFAA guidelines mentioned above clearly indicate that threats to public health are priorities for CFAA prosecution,[95] so the government may be eager to try a test case.

Much writing on the CFAA has focused on the idea that, as a fairly broad statute, it over-criminalizes behavior which, while perhaps not innocuous, should also not be criminal.[96] Proponents

---

92. *E.g.*, 40 C.J.S. *Homicide* § 127 (2018) ("Involuntary manslaughter is committed when a person, *while engaged in an unlawful act, unintentionally causes the death of another* or where a person engaged in a lawful act unlawfully causes the death of another.") (emphasis added).

93.

> Defendant asserts that insufficient evidence was presented to support her involuntary manslaughter conviction based on her failure to perform a legal duty as there is no specific legal duty to "safeguard, control and prevent the discFharge of a loaded firearm." We disagree.
>
> This conclusion is based on testimony that defendant had a loaded gun in her hand as she tried to let herself in the house, that the victim was only a few feet away from defendant, and that the gun somehow fired, hitting the victim in the face. Sufficient evidence was presented so that the jury could have inferred that it would be apparent to the ordinary mind that failure to perform a legal duty to safeguard, control and protect the loaded gun was likely to prove disastrous to the victim.

People v. Weaks, No. 183697, 1996 WL 33357539 (Mich. Ct. App. Sept. 27, 1996).

94. Jesse M. Ehrenfeld, *WannaCry, Cybersecurity and Health Information Technology: A Time to Act*, 41 J. MED. SYS. 104, 104 (2017); *see also* Filip Truta, *New Ransomware Attack Forces Hospitals to Turn Away Patients*, HOT FOR SEC. (Jan. 25, 2018, 3:41 PM), https://hotforsecurity.bitdefender.com/blog/new-ransomware-attack-forces-hospitals-to-turn-away-patients-19490.html (describing how some hospitals are refusing to treat patients because their electronic health records system were shut down by ransomware).

95. Attorney General Memorandum, *supra* note 89.

96.

> The government's construction . . . . [makes] criminals of large groups of people who would have little reason to suspect they are committing a

of the CFAA often point to prosecutorial discretion as a solution to this problem,[97] but detractors in turn point to cases where prosecutors arguably overstepped.[98] Additionally, since the CFAA created a private right of action,[99] prosecutorial discretion simply has no role in many cases. For this reason, the rule of lenity[100] has been invoked in the context of the CFAA,[101] but has had little to no actual effect in narrowing the breadth with which the statute is interpreted.[102]

III. ANALYSIS

A. HOW WELL WOULD ANY OF THESE APPROACHES ACTUALLY WORK?

Each of the above approaches to assigning responsibility in the context of vulnerability disclosure has worth, but some are likely to have more of a positive impact than others. The adoption of a negligence framework is perhaps one of the more likely scenarios for further control of vulnerability disclosure, as

---

> federal crime . . . . Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.

United States v. Nosal (*Nosal I*), 676 F.3d 854, 859–60 (9th Cir. 2012), *overruled by* United States v. Nosal (*Nosal II*), 844 F.3d 1024 (9th Cir. 2016) (holding that the CFAA applies to misappropriation); Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology ("The Justice Department's interpretation [of the CFAA] makes the American desk-worker a felon.").

97. *Nosal I*, 676 F.3d at 862 ("The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations.").

98. *Id.* (quoting United States v. Stevens, 559 U.S. 460, 480 (2010)) ("The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't have to live at the mercy of our local prosecutor . . . ' We would not uphold an unconstitutional statute merely because the government promised to use it responsibly.'"); MCGEVERAN, *supra* note 85, at 473 ("[T]here certainly are examples where federal prosecutors used CFAA charges to go after persons who may have been in their sights notwithstanding any hacking allegations.").

99. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2012).

100. *Nosal I*, 676 F.3d at 863 (quoting United States v. Witberger, 18 U.S. 76, 95 (1820)) ("The rule of lenity requires 'penal laws . . . to be construed strictly.'").

101. *E.g.*, *id.*

102. *E.g.*, United States v. Nosal (*Nosal II*), 844 F.3d 1024, 1035 n.6 (declining to apply the rule of lenity due to a perceived lack of ambiguity in the CFAA, despite acknowledging a narrower interpretation of the CFAA exists).

negligence is an extraordinarily wide-ranging concept which has been adapted to virtually every corner of modern American life.[103] Data breach litigation, for example, is a growing field of negligence actions against companies holding consumer data.[104] Malware researchers are already sued or threatened with litigation somewhat frequently,[105] and expanding negligence to encompass allegedly improper vulnerability disclosure runs the risk of chilling the enthusiasm of security researchers to research and disclose vulnerabilities,[106] and of pushing them towards anonymous or black market disclosures.[107]

Negligence actions are an attractive proposition for dealing with the problem of improper disclosure because courts are very aware of how negligence works and an entirely new framework may prove to be more confusing than an approach which merely introduced new duties, or new ways to breach existing duties, to the existing negligence framework. Adopting this framework would give courts a straightforward means of treating malware researchers as professionals who have adopted a set of professional standards. Even though the development and adjustment of those standards is—and will continue to be—difficult, professional organizations and other groups with

---

103. HENDERSON, PEARSON & KYSAR, *supra* note 48, at 159.

104. *See, e.g.*, *In re* The Home Depot, Inc., Customer Data Security Breach Litig., MDL Docket No. 2583, 2016 WL 2897520, at *3–5 (N.D. Ga. 2016) (discussing negligence law in the context of a data breach); *In re* Premera Blue Cross Customer Data Security Litig., 198 F. Supp. 3d 1183 (D. Or. 2016).

105. *Legal Threats Against Security Researchers*, ATTRITION, http://attrition.org/errata/legal_threats/ (last visited Apr. 9, 2018) (providing summaries of recent legal action against security researchers, and strongly advocating that most such actions are baseless attempts to save face).

106. Malena Carollo, *Influencers: Lawsuits to Prevent Reporting Vulnerabilities Will Chill Research*, CHRISTIAN SCI. MONITOR: PASSCODE (Sept. 29, 2015), https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2015/0929/Influencers-Lawsuits-to-prevent-reporting-vulnerabilities-will-chill-research.

107. *See* Zack Whittaker, *Lawsuits Threaten Infosec Research—Just When We Need It Most*, ZDNET (Feb. 19, 2018, 5:00 PM), http://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/ ("One independent researcher, who asked not to be named, said that they will 'simply post details of a flaw anonymously online' [due to fear of litigation]."); *see also* Carollo, *supra* note 106 ("'Numerous researchers have either stopped looking for bugs, or worse, have stopped reporting them. The bugs are still there, possibly being used by the bad guys, but fear of prosecution, for what amounts to telling the truth, stops many researchers from reporting bugs.'").

expertise are better at this work than courts are,[108] and courts will benefit from the input of these groups every time an expert witness testifies at trial. Medical malpractice cases already delegate this responsibility to expert witnesses: "The overwhelming weight of authority supports the view that ordinarily expert evidence is essential to support an action for malpractice against a physician or surgeon."[109] Allowing expert witnesses and professional organizations to set the standards of malware research could decrease the work required by courts and would likely result in law which better reflects the professional standards actually adopted by industry. Other elements of negligence, such as causation, are also highly likely to require expert testimony in technologically complex cases.[110]

On the other hand, negligence actions may not be the best way to handle vulnerability disclosure, simply because malware researchers typically have fewer financial resources and less in-house legal capacity compared to the companies whose products they research.[111] This asymmetry means some tech companies may bully well-meaning and responsible researchers into silence through threats of meritless litigation. Recourse does exist in other areas of the law for defendants of meritless litigation, such as fee-shifting measures[112] and anti-SLAPP laws,[113] but even if

---

108. Many organizations are already engaged in crafting similar systems of voluntary standards. *See, e.g.*, NAT'L. INST. OF STANDARDS & TECH., *supra* note 50; 6 U.S.C. §§ 1501–10 (2012). *But see* Kesan & Hayes, *supra* note 21, at 776 ("Some critics question the wisdom of even voluntary cybersecurity standards, due to the risk that companies will adopt the bare minimum required to comply. Providing a higher baseline than what might have existed before is valuable, but the danger comes when agencies mistake practices that are necessary to improve security, and practices that are sufficient to improve security.").

109. H. H. Henry, Annotation, *Necessity of Expert Evidence to Support an Action for Malpractice Against a Physician or Surgeon*, 81 A.L.R. 2d 597 Art. 1, § 2 (1962).

110. Causation in particular has played a large role in other cybersecurity cases. *E.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317, 1331–32 (11th Cir. 2012) (Pryor, J., dissenting) (arguing that plaintiffs alleged only correlation, rather than causation).

111. *See, e.g.*, Whittaker, *supra* note 107 (documenting the chilling effect of legal threats on security researchers).

112. *See* Jessica Erickson, *Heightened Procedure*, 102 IOWA L. REV. 61, 70–74 (2016) (discussing cost asymmetry in litigation, as well as fee-shifting laws and other means of accounting for cost asymmetry).

113. For a discussion of Anti-SLAPP statutes in general, and for a discussion of California's Anti-SLAPP statute in particular, see Brian D. Shaffer, *California's Anti-SLAPP Statute: A Potent, Yet Confounding, Weapon*, 27 MILLER & STARR REAL EST. NEWSALERT 589 (2017).

a cybersecurity law expressly applied such recourse to the vulnerability disclosure context, securing such recourse would itself require an investment, which small companies or individuals may not be able to afford.[114] Taking into account, as noted above, that some tech companies have already sued malware researchers in what may be attempts to silence criticism of their products,[115] the expansion of negligence to encompass allegedly improper vulnerability disclosure may be unwise, since it provides additional grounds for litigation which may be baseless. Finally, encouraging negligence actions as the primary means for addressing improper vulnerability disclosure may have a negative impact on the development of the law, simply because the development of case law is typically a long process.[116] While courts develop the case law on improper vulnerability disclosure over what may be decades, the industry may be left with frustrating uncertainty as to what the rules actually are.

Adopting a strict liability analysis of vulnerability disclosure may be an appealing alternative to general negligence, but if it were to be adopted, it should be greatly constrained to a miniscule subset of vulnerability disclosure which is truly "abnormally dangerous."[117] The Restatement definition of "abnormally dangerous" is confined to uncommon activities which "[create] a foreseeable and highly significant risk of physical harm even when reasonable care is exercised by all actors."[118] In applying this definition to vulnerability disclosure, it's important to keep in mind that most vulnerability research is probably not uncommon in the sense necessary to

---

114. For an in-depth analysis of the cost and process of fighting malicious or frivolous lawsuits in states both with and without anti-SLAPP legislation, see Ken White, *Why, Yes, I AM Into SLAPPing*, POPEHAT (June 7, 2012), https://www.popehat.com/2012/06/07/why-yes-i-am-into-slapping/.

115. *Legal Threats Against Security Researchers*, *supra* note 105.

116. *See* Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 8 (2007) (noting that between Warren and Brandeis's conception of the privacy torts and Dean Prosser's solidification of them, 70 years passed).

117. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 (AM. LAW INST. 2010). Notably, there are other activities in addition to those that are "abnormally dangerous" in which strict liability can be applied to a certain situation, including, for example, possessing exotic or dangerous pets. *Id.* §§ 22–23.

118. *Id.* § 20.

meet this definition.[119] Additionally, the requirement of "physical harm" probably forecloses the vast majority of these cases, since any harm caused by improper disclosure is overwhelmingly unlikely to be physical. Third, "reasonable care," properly defined, is likely to foreclose the possibility of significant harm.

Because it may not be intuitive that reasonable care has that effect, an example may be provided by examining the Shadow Brokers leak discussed at the beginning of this Note.[120] Shadow Brokers disclosed massive amounts of information about zero-day exploits and other cyberweapons, including EternalBlue, to the public without first contacting Microsoft, the NSA, or any other parties.[121] This is clearly a violation of reasonable care, because reasonable security researchers generally don't do any of the following: A) break into and steal information from government databases,[122] B) publicly release volatile information without contacting vendors or other impacted parties (in this case, Microsoft) to mitigate the harm which could follow such a release,[123] or C) fail to redact or delay such information in any manner.[124] Shadow Brokers involved themselves in incredibly dangerous activities which resulted in massive consequences, but those activities were dangerous *because* Shadow Brokers failed to exercise reasonable care, rather than *despite* their exercise of reasonable care. A likelihood of serious consequences *despite* reasonable care is the linchpin of

---

119. This is a somewhat complex question to analyze but consider one metric: approximately 80,000 Americans hold Certified Information Systems Security Professional (CISSP) qualifications. This common information security certificate requires expertise comparable to the level of expertise needed to carry out vulnerability research. *(ISC)² Member Counts*, (ISC)² (Jan. 1, 2018), https://www.isc2.org/About/Member-Counts.

120. Goodin, *supra* note 6.

121. *Id.*

122. This behavior is clearly delineated as unreasonable by both the letter and the spirit of the CFAA. 18 U.S.C. § 1030(a)(2)(b) (2012). To clarify—"break into" implies a lack of authorization or some practice that goes beyond existing system authorization, even though authorization in a different sense may exist for this behavior given other facts. For instance, a penetration testing company could secure authorization to attempt to break into the DOJ's computer system without violating the CFAA.

123. Existing norms and existing Responsible Disclosure policies render this unreasonable. *See, e.g.*, Bonderud, *supra* note 63.

124. This is also rendered unreasonable by Responsible Disclosure norms and policies. *See, e.g.*, *id.*

strict liability,[125] and because a reasonable standard of care in cybersecurity can go a long way to prevent serious consequences, strict liability will typically be an inappropriate analysis in the context of vulnerability disclosure.[126]

One specific facet of Shadow Brokers is perhaps more interesting than others in the context of strict liability: Shadow Brokers stole a stockpile of information and cyberweapons from the NSA, and they released that information in large "dumps," which can fairly be regarded simply as public stockpiles.[127] Some groups, including Microsoft[128] and advisory entities within the Obama Administration,[129] have questioned the general concept of stockpiles, and have argued a point similar to a strict liability analysis—cyber-weapons stockpiles are dangerous things, even when great care is exercised.[130] Some entities in the research community have pushed back on the criticism of stockpiles. Malpedia is one example of a fairly large stockpile of malware, much of it unpatched and dangerous, which is maintained and used for research purposes.[131] Malpedia is "operated as an invite-only trust group"—meaning access to the stockpile is limited to researchers known to its operator as trustworthy.[132] Assuming that a duty exists to responsibly limit access to dangerous cyberweapons only to those parties who would not reasonably be expected to use the information maliciously, Malpedia fulfills that duty better than Shadow Brokers, who did

---

125. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 (AM. LAW INST. 2010).

126. Creating a hypothetical in which strict liability would be appropriate is difficult, but one example of the rare scenarios in which strict liability would be the appropriate analysis follows: imagine a penetration testing company, hired to test the security and operability of systems which regulate a running nuclear reactor (assume that it is not possible to test the programs while the reactor has been safely shut down). Even with the highest conceivable standard of care, this test is absolutely an abnormally dangerous activity, because even though the risk is low, successful penetration could have catastrophic consequences if some critical system function was altered because of the testing.

127. Goodin, *supra* note 6.

128. Smith, *supra* note 10.

129. THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE & COMMC'NS TECHS., *supra* note 18; *see also* Brandom, *supra* note 18.

130. THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE & COMMC'NS TECHS., *supra* note 18.

131. *Malpedia*, FRAUNHOFER FKIE, https://malpedia.caad.fkie.fraunhofer.de/ (last visited Apr. 9, 2018).

132. *Malpedia Terms of Service*, FRAUNHOFER FKIE, https://malpedia.caad.fkie.fraunhofer.de/terms_of_service (last visited Apr. 16, 2018).

not restrict access to their dump at all. However, Malpedia's security infrastructure is almost certainly weaker than the NSA's—and as Shadow Brokers made all too clear, even the NSA is not invulnerable.[133]

Criminal law will likely remain relevant in this area. Despite substantial criticism of the CFAA,[134] the DOJ has released memoranda which appear to indicate that CFAA prosecutions will continue.[135] Specifically, the most recent memorandum indicates that the DOJ is interested in trying a CFAA case in which a risk of bodily harm existed.[136] In the context of recent threats to hospital and healthcare systems,[137] this may indicate that the DOJ would be willing to try a case in which, for instance, ransomware shut down a system which was directly responsible for sustaining a patient's life.

Despite this sustained enthusiasm on the part of the DOJ,[138] a scenario in which the CFAA is either replaced or heavily amended is likely to be much more palatable to many scholars.[139] Kirsch argues that "all hacking is essentially illegal under the [CFAA]," that "the CFAA has become so broad that the law now 'threatens to swallow the Internet,'" and that "the broad language of the CFAA is a result of out-dated Internet philosophies from before the Internet's omnipresence in society."[140] The central problem with the CFAA is likely that the concept of "unauthorized access" is immensely broad and nebulous,[141] which may lend itself to excessive prosecutorial discretion.[142] In order to address these problems, a new and

---

133. Goodin, *supra* note 6; *see also* Smith, *supra* note 10.

134. *See* McLaughlin, *supra* note 90.

135. Attorney General Memorandum, *supra* note 89.

136. *Id*.

137. *See* Ehrenfeld, *supra* note 94; Truta, *supra* note 94.

138. This enthusiasm may not always be shared by the companies on whose behalf the DOJ brings criminal charges. *See* Kerr, *supra* note 58, at 1170 ("It is telling that when the government has pursued aggressive criminal charges under the CFAA for use of websites, it has often been without the support of the companies claimed as victims.").

139. *See* McLaughlin, *supra* note 90; *see also* Kerr, *supra* note 58.

140. Kirsch, *supra* note 80, at 392–93.

141. Fidler, *supra* note 19, at 68, ("The CFAA has been criticized for its 'breadth and severity.' The law has increasingly been used to prosecute offenses . . . one might not consider classical hacking.").

142. *See* Kesan & Hayes, *supra* note 21, at 771 ("[S]ome question the government's enforcement patterns. A majority of referred CFAA cases are left unprosecuted due to lack of evidence, while CFAA prosecutions that do go

modern cybercrime law could adopt language substantially different from "unauthorized access" to describe criminal usage of a computer, language could be added to the CFAA through amendment or judicial interpretation which clearly delineates what "unauthorized access" means, or the DOJ could work with industry groups to discuss possible amendments to the prosecutorial guidelines, aimed at criminalizing only detrimental "unauthorized access."[143] The modern world is one in which certain kinds of hacking should be perfectly legal. The CFAA needs to be reinterpreted or amended in order to better reflect that view, and until it is, criminal law in the area of cybersecurity will be significantly outdated.[144]

Other possible approaches do exist, including Kesan & Hayes' market approach[145] and the Dual-Use Research of Concern (DURC) approach used in biohazard research and in the Wassenaar Agreement.[146] The market approach is probably unhelpful, if only because it may pose another barrier to entry into tech—an industry which depends heavily on startups. Bugs are common in all software, and many start-ups would have an incredibly difficult time justifying to investors a seven-figure budget for buying all the bugs in their software. DURC is also

---

forward sometimes play fast and loose with what it means to access a computer without authorization . . . . [I]nconsistent applications of [CFAA] threaten to discourage benevolent security research while encouraging the actions of malicious hackers who know that their odds of being caught and prosecuted are slim.").

143. One polarizing issue on this final point may be the prosecution and subsequent suicide of Aaron Swartz, an internet activist who was charged under the CFAA after he downloaded several million academic journals articles. McLaughlin, *supra* note 90; Larissa MacFarquhar, *Requiem for a Dream*, NEW YORKER (Mar. 11, 2013), https://www.newyorker.com/magazine/2013/03/11/requiem-for-a-dream. Discussions about Swartz illustrate the human cost of uncertainty regarding the bounds of the CFAA.

144. *See* Kirsch, *supra* note 80, at 392–93 (arguing the CFAA is outdated); Orin Kerr, *Obama's Proposed Changes to the Computer Hacking Statute: A Deep Dive*, WASH. POST: THE VOLOKH CONSPIRACY (Jan. 14, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/?utm_term=.905180db351b ("The law is a mess, yes. And there are some frightening readings of the law that courts might adopt under the current text . . . [but] I'm relatively optimistic that the narrower readings will prevail if and when the Supreme Court turns to the CFAA.").

145. *See* Kesan & Hayes, *supra* note 21, at 817–29.

146. *See* Imperiale & Casadevall, *supra* note 42, at 2–4 (discussing DURC in biohazard research); Fidler, *supra* note 19, at 135 (discussing the Wassenaar Agreement).

probably inappropriate, for three reasons: A) no analogous oversight mechanism to the NIH exists in information security, even though some systems like NIST do provide voluntary standards, B) DURC in the biotechnology field functions largely through threats of removing federal funding,[147] threats which cannot be applied to private tech companies and private malware researchers, and C) a dual-use analysis was already attempted in the context of vulnerabilities with the Wassenaar Agreement, which has gone essentially nowhere.[148]

B. WHAT STANDARDS SHOULD ULTIMATELY ATTACH TO VULNERABILITY RESEARCHERS AND ADJACENT INDUSTRIES?

Industry groups and other stakeholders are likely the most qualified individuals to discuss the specific duties incumbent on malware researchers. With that in mind, Responsible Disclosure[149] is likely the standard which has the most support of individuals and organizations in the information security industry.[150] Responsible Disclosure is also desirable because it would integrate well with common law negligence, since authorship on Responsible Disclosure tends to clearly delineate the respective duties of security researchers and companies.[151] Through adopting the considered analysis and thought of many information security scholars, courts are likely to come to a much more accurate conception of the standard of care owed by vulnerability researchers. Responsible Disclosure has historically had some problems with providing an appropriate incentive to malware researchers, especially when compared to the black market,[152] so other means of encouraging Responsible Disclosure should be developed. These might include federal subsidies or tax incentives for bug bounties, immunity from related IP infringement or CFAA cases,[153] or other incentives.

---

147. Imperiale & Casadevall, *supra* note 42, at 3.

148. Kesan & Hayes, *supra* note 21, at 777.

149. *See* Bonderud, *supra* note 63.

150. Google Security Team, *supra* note 31.

151. *See, e.g.*, *id.*

152. *See, e.g.*, Kesan & Hayes, *supra* note 21, at 761.

153. *See*, *e.g.*, *id.* at 803 (citing Derek E. Bambaeur & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1086 (2011)) ("Bambauer and Day, for example, recommend granting researchers immunity from intellectual property litigation if they follow a responsible disclosure model.").

Even if Responsible Disclosure were to be adopted, it only covers so much ground, and leaves many questions unanswered—for instance, what level of access restriction should we consider "responsible" when managing a stockpile of cyberweapons? Shadow Brokers is certainly irresponsible in their total lack of restriction, but is Malpedia[154] irresponsible because they operate a stockpile of unpatched malware despite lacking resources comparable to a branch of the largest military on the planet?[155] Is the NSA irresponsible because their security was breached despite presumably using those resources wisely? Ideally, the answers to these questions would correspond to a sliding scale, in which the level of requisite protection corresponds to the apparent danger posed by the material stockpiled. This is somewhat a common sense approach: most people would consider someone a responsible weapon custodian if she locked a gun in a well-built safe, but not if she locked a nuclear weapon in the same safe.

Confusingly, however, analyses using such a sliding scale may conclude that Malpedia responsibly protects their stockpile while the NSA did not, even if the NSA had invested more in security infrastructure and created an environment which was overall much more secure than Malpedia's. Additionally, a sliding scale approach may create difficulties when a particular piece of malware poses an uncertain danger. If a security researcher quarantines a suspicious file from a spam e-mail and uploads it to a service like Malpedia for further research without realizing that the file contains a highly engineered cyberweapon utilizing a handful of kernel-level zero-day exploits in Windows, that security researcher may have unwittingly catapulted the service's obligation to restrict access to a much higher level (if the sliding scale proposed depends only on what the service actually holds, rather than on what they *know*—constructively or otherwise—they hold). In such a situation, the sliding scale rule would a) likely fail to provide adequate limits on access to the malware, and simultaneously b) unfairly impose an extremely high obligation on an unwitting service, despite that service's reasonable belief that they were fulfilling their security obligations. The latter may be "solved" by adapting the rule to

154. *Malpedia*, *supra* note 131.

155. *What We Do: Support to the Military*, NAT'L SEC. AGENCY (May 3, 2016), https://www.nsa.gov/what-we-do/support-the-military/ ("The National Security Agency is part of the U.S. Department of Defense.").

adjust protection in accordance with the service's reasonable expectation of the danger imposed by their stockpile, but such a change would probably fail to inspire any sense of certainty. As to the former, there is probably no satisfying solution.

IV. CONCLUSION

Shadow Brokers and groups like them, who carelessly disclose the practical equivalent of a weapon to the public at large without sufficient care, must be held responsible for their carelessness. As discussed above, this is possible under a variety of approaches. The CFAA provides a great deal of power and discretion to prosecutors, for example, but such discretion may be misapplied in less clear-cut cases. Because of the uncertainty in the CFAA's application, civil actions such as negligence are a better way to address alleged wrongs in the context of vulnerability disclosure, especially when industry experts are allowed to testify as to critical aspects of the case, such as duty. Responsible Disclosure and similar doctrines could be determinative in such cases. These doctrines can gain legal weight two ways. First, they may be incorporated into the common law through inclusion in judicial opinions after trials at which expert witnesses testified. Second, states or the U.S. Government may pass statutes requiring researchers to meet Responsible Disclosure standards, which would thereby render non-compliant researchers per se negligent. Widespread adoption of industry standards like Responsible Disclosure, coupled with allowance for continued industry input to courts and other decision-makers regarding updates to those standards, is in the best interest of everyone involved in vulnerability disclosure.

***